



# KOREAN PATENT ABSTRACTS(KR)

Document Code: A

(11) Publication No. 1020000012194 (43) Publication Date. 20000306

(21) Application No. 1019990024771 (22) Application Date. 19990628

(51) IPC Code:

G06F 17/00

(71) Applicant:

CYBER TEC HOLDINGS CO., LTD.

(72) Inventor:

KIM, HYEONG TAE

YOO, BU IL

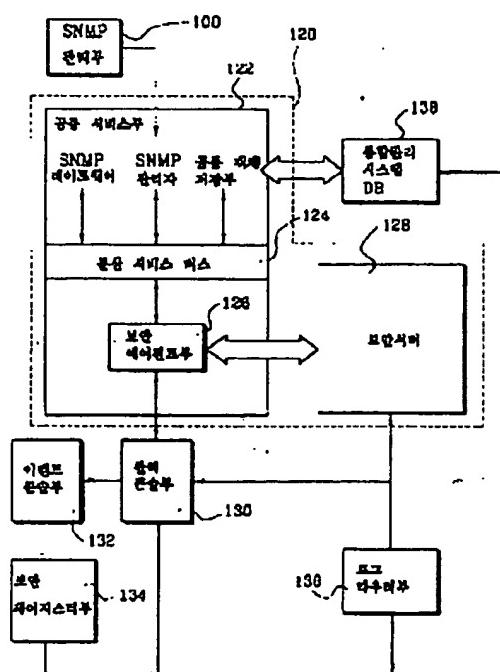
(30) Priority:

(54) Title of Invention

SYSTEM FOR UNIFYING SYSTEM MANAGEMENT SYSTEM AND FIREWALL SYSTEM

Representative drawing

(57) Abstract:



PURPOSE: A system for unifying a system management system and a firewall system is to install four modules in the place which a system management system or a firewall system is located and operates four modules each other for unifying and managing two systems.

CONSTITUTION: A system comprises: a firewall agent unit (126) for generating a trap event when an abnormality is occurred in the firewall system and providing the information to resources related to the network firewall; a firewall register unit for storing the information related to the network firewall in a common database of the system management system and the firewall system and performing a deletion, an amendment or an access; a log router unit for reading log information from the firewall system to analyze and providing an urgent message or a SNMP trap message to an event console of the system management system; and a management console unit for managing the log router unit and the firewall resistor unit. Thereby, an effective management of the resource and a reliable circumstance to users are provided, the circumstance independently operating the network firewall system and the system management system.

firewall resistor unit. Thereby, an effective management of the resource and a reliable circumstance to users are provided, the circumstance independently operating the network firewall system and the system management system.

COPYRIGHT 2000 KIPO

if display of image is failed, press (F5)

## (19) 대한민국특허청(KR)

## (12) 공개특허공보(A)

|   |                        |                              |
|---|------------------------|------------------------------|
| (51) Int. Cl.<br>G06F 17/00(조기공개)   | (11) 공개번호<br>(43) 공개일자 | 특2000-0012194<br>2000년03월06일 |
| (21) 출원번호<br>10-1999-0024771  |                        |                              |
| (22) 출원일자<br>1999년06월28일  |                        |                              |
| (71) 출원인<br>주식회사 싸이버텍홀딩스, 김상배<br>대한민국<br>150-010<br>서울특별시 영등포구 여의도동 45-11 신한빌딩 3층                                       |                        |                              |
| (72) 발명자<br>김형태<br>대한민국<br>449-840<br>경기도 용인시 수지읍 440번지<br>유부일<br>대한민국<br>421-160<br>경기도 부천시 오정구 내동 54-47/5 서울주택 가동 12호 |                        |                              |
| (74) 대리인<br>이영필<br>권석율<br>이상용   |                        |                              |
| (77) 심사청구<br>있음   |                        |                              |
| (54) 출원명<br>통합관리시스템과 보안시스템을 통합하기 위한 시스템   |                        |                              |

## 요약

본 발명은 통합관리시스템과 보안시스템을 통합하기 위한 시스템에 관한 것이다. 그 시스템은, 보안시스템의 네트워크 보안에 관련된 자원들의 상태를 감시하고, 정보를 수집하여 저장하며, 상기 보안시스템에 이상이 발생한 경우 트랩 이벤트를 발생하고, 상기 통합관리시스템의 요청에 따라 상기 네트워크 보안 관련 자원들에 대한 정보의 제공 또는 프로세스를 제어하기 위한 보안 애이전트부; 네트워크 보안에 관련된 정보를 상기 통합관리시스템과 보안시스템의 공통 데이터 베이스에 저장하고, 상기 저장된 정보의 삭제, 수정 및 조회를 수행하기 위한 보안 레지스터부; 상기 보안시스템으로부터 접속 시도에 대한 기록을 나타내는 로그 정보(Log Information)를 가져와서 분석하고, 문제가 있는 경우 긴급 메시지 또는 SNMP(Single Network Management Protocol) 트랩 메시지를 통합관리시스템의 이벤트 콘솔(Event Console)로 제공하기 위한 로그 라우터부; 및 상기 SNMP를 사용하여 상기 보안시스템을 감시하며, 상기 보안 관련 정보를 가져와서 상기 보안시스템의 상태를 감시하고, 상기 보안 관련 정보 및 프로세서 제어를 상기 보안 애이전트부로 요청하며, 상기 로그 라우터부 및 상기 보안 레지스터부를 관리하기 위한 관리콘솔부를 포함함을 특징으로 한다. 본 발명에 따르면, 사용자에게 지원의 효율적인 관리와 신뢰성 있는 사용환경을 제공할 수 있다.

## 대표도

도 1

명세서

## 도면의 간단한 설명

도 1은 본 발명의 바람직한 실시예에 따른 통합관리시스템과 보안시스템을 통합하기 위한 시스템의 블록도이다.

도 2는 보안 애이전트부의 동작을 설명하는 흐름도이다.

도 3은 로그 라우터부의 동작을 설명하는 흐름도이다.

도 4에 관리 콘솔부의 동작을 설명하는 흐름도이다.

## 발명의 상세한 설명

## 발명의 목적

## 발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 통합관리시스템(System Management System)과 보안시스템(Firewall System)을 통합하기 위한 시스템에 관한 것으로, 보다 상세하게는 상호 독립적으로 동작할 수 있는 4개의 모듈을 통합관리시스템 또는 보안시스템이 위치한 곳에 설치하여 상기 모듈들이 상호 작용하도록 함으로써 두 시스템을 통합하여 관리할 수 있도록 한 통합관리시스템과 보안시스템을 통합하기 위한 시스템에 관한 것이다.

최근 들어 클라이언트/서버 구축술이 기업 컴퓨팅계에 보급되면서, 분산된 시스템들을 관리하는 문제가 갈수록 중요성을 더해가고 있으며, 여기에 통신과 원격접속, 인수, 학병 등이 이러한 움직임을 부추기고 있다.

통합관리시스템(System Management System)이란 기업내에서 여기저기 분산되어 있는 시스템, 네트워크, 애플리케이션 등을 통합하여 관리할 수 있도록 하는 시스템(소프트웨어)을 말한다. 보안시스템(Firewall System)은 외부 네트워크와 내부 네트워크의 경계선에 위치하여 외부 패킷이 내부 네트워크로 침입하는 것을 차단하는 시스템이다.

한편, 현재의 통합관리시스템은 네트워크 자원을 관리하기 위하여 원격에서 시스템을 관리하는 프로토콜을 이용하여 시스템의 동작여부를 체크하는 단순한 프로세스 관리수준의 지원방식이다. 따라서, 고유의 룰들이 제공하는 다양한 기능들을 충분히 수용할 수 없다는 문제점이 있다. 또한, 최근에는 보안이 중요한 이슈로 등장하여 관련 자원에 대한 상세한 정보와 문제가 요구됨으로써 이를 보완하여야 하는 요구가 증대하고 있다. 그러나, 기존의 통합관리영역에서 자원관리가 보안에 대하여 경증되지 않은 인터페이스를 제공하여 보안에 대한 또 다른 문제점을 야기함으로써 이를 보완해야 필요가 대두되어 왔다.

### 발명이 이루고자 하는 기술적 과제

본 발명의 목적은 상기의 문제점을 해결하기 위해, 상호 독립적으로 동작할 수 있는 4개의 모듈을 통합관리시스템 또는 보안시스템이 위치한 곳에 설치하여 상기 모듈들이 상호 작용하도록 함으로써 두 시스템을 통합하여 관리할 수 있도록 한 통합관리시스템과 보안시스템을 통합하기 위한 시스템을 제공하는 것이다.

### 발명의 구성 및 작용

상기의 목적을 달성하기 위하여,

통합관리시스템(System Management System)과 보안시스템(Firewall System)을 통합하기 위한 시스템에 있어서,

상기 보안시스템의 네트워크 보안에 관련된 자원들의 상태를 감시하고, 정보를 수집하여 저장하며, 상기 보안시스템에 이상이 발생한 경우 트랩 이벤트를 발생하고, 상기 통합관리시스템의 요청에 따라 상기 네트워크 보안 관련 자원들에 대한 정보의 제공 또는 프로세스를 제어하기 위한 보안 에이전트부; 네트워크 보안에 관련된 정보를 상기 통합관리시스템과 보안시스템의 공통 데이터 베이스에 저장하고, 상기 저장된 정보의 삭제, 수정 및 조회를 수행하기 위한 보안 레지스터부; 상기 보안시스템으로부터 접속 시도에 대한 기록을 나타내는 로그 정보(Log Information)를 가져와서 분석하고, 문제가 있는 경우 긴급 메시지 또는 SNMP(Single Network Management Protocol) 트랩 메시지를 통합관리시스템의 이벤트 콘솔(Event Console)로 제공하기 위한 로그 라우터부; 및 상기 SNMP를 사용하여 상기 보안시스템을 감시하며, 상기 보안 관련 정보를 가져와서 상기 보안시스템의 상태를 감시하고, 상기 보안 관련 정보 및 프로세서 제어를 상기 보안 에이전트부로 요청하며, 상기 로그 라우터부 및 상기 보안 레지스터부를 관리하기 위한 관리콘솔부를 포함하며, 상기 보안 에이전트부, 보안 레지스터부, 로그 라우터부 및 관리 콘솔부는 통합관리시스템에서 제공하는 인터페이스 프로그램과 관련된 관리용 인터페이스를 위한 코드 또는 네트워크 보안 시스템의 인터페이스를 위한 코드를 포함함을 특징으로 하는 통합관리시스템과 보안시스템을 통합하기 위한 시스템이 제공된다.

이하, 첨부된 도면들을 참조하여 본 발명의 실시예를 상세히 설명하기로 한다.

도 1은 본 발명의 바람직한 실시예에 따른 통합관리시스템과 보안시스템을 통합하기 위한 시스템의 블록도이다.

도 1에 도시된 시스템에서, 참조부호 100은 SNMP(Single Network Management Protocol) 관리부를, 120은 보안시스템이 설치된 위치를, 참조부호 132~138은 통합관리시스템측에 설치되는 블록들을 각각 나타낸다.

SNMP 관리부(100)는 SNMP를 관리하는 애플리케이션이다. 여기서, SNMP(Single Network Management Protocol)는 네트워크를 관리하는 가장 일반적인 네트워크 관리 프로토콜이다. 통상, SNMP는 관리자의 물음에 대리인(Agent)이 응답하는 것이 기본이고, 대리인은 특수한 상황이 발생한 경우에 관리자에게 발생을 알리고 필요한 정보를 함께 보낸다.

공통 서비스부(122)는 SNMP 게이트웨이, SNMP 관리자/Administrator) 및 공통 객체 저장부(Common Object Repository)를 포함하며, 분산 서비스 버스(Distributed Service Bus: 124)를 통해 보안 에이전트부(126)와 상호 통신한다. 공통 객체 저장부는 통합관리시스템과 보안시스템의 공통 데이터를 저장하기 위한 데이터 베이스이다.

통합관리시스템 DB(138)는 통합관리시스템 관리에 필요한 데이터 베이스이다.

보안 서버(128)는 보안시스템을 설치하여 기업/기관의 보안을 전반적으로 관리하고 제어하기 위한 서버이다.

이벤트 콘솔부(Event Console: 132)는 통합관리시스템에서 각종 정보들의 진행 상황에 대한 정보 및 경고, 오류 등에 대한 메시지를 취합하는 모듈이다. 이는 다양한 이벤트나 메시지를 한 곳으로 집중시킴으로써 관리자들에게 보다 편의적인 환경을 제공할 수 있게 해준다.

보안 에이전트부(Firewall Agent: 126)는 보안시스템의 네트워크 보안에 관련된 자원들의 상태를 감시하고, 정보를 수집하여 저장하며, 상기 보안시스템에 이상이 발생한 경우 트랩 이벤트(Trap Event)를 발생하고, 통합관리시스템의 요청에 따라 상기 네트워크 보안 관련 자원들에 대한 정보의 제공 또는 프로세스를 제어한다.

보안 에이전트부(126)는 네트워크상에 분산되어 있는 네트워크 보안에 관련된 여러 자원들이 설치되어 있는 위치에 배치되어 동작하는 프로그램 모듈이다.

도 2에 보안 에이전트부(126)의 동작을 설명하는 흐름도가 도시되어 있다.

시스템 서비스/데몬 형식 또는 사용자의 직접 명령에 의해 프로그램을 시작한다.(202 단계)

수행하는 서비스 종류가 무엇인지를 체크한다.(204 단계) 즉, 모듈이 처음 시작되면, 해당 서비스를 수행하기 위하여 각각의 서비스를 별도의 프로세서로 진행하기 위하여 분기한다.

서비스가 정보 수집 및 저장 서비스인 경우에, 주기적으로 네트워크 보안에 관련된 상태의 감시 및 정보를 수집한다.(206 단계)

수집된 정보를 공통 객체 저장부에 저장한다.(208 단계) 이는 수집된 정보를 별도의 장소에 보관하여 추후 사용할 수 있도록 하기 위함이다.

트랩 이벤트 발생 서비스인 경우에는, 네트워크 보안에 관련된 상태에 변화가 발생하였는지 판단한다.(210 단계) 변화가 발생한 경우에는 트랩 이벤트를 발생한다.(212 단계) 이는, 네트워크 보안 관련 상태에 문제 발생시 트랩 이벤트를 발생함으로써 관리자가 이에 대해 적절한 조치를 취할 수 있도록 하기 위함이다.

관리 콘솔부(Management Console: 130)로 제공하기 위한 서비스인 경우에는, 관리 콘솔부(130)로부터의 서비스 요청을 기다린다.(214 단계)

관리 콘솔부로부터의 서비스 요청이 오면, 해당 요청에 대한 서비스를 제공하기 위한 별도의 프로세스를 생성한다.(216 단계) 물론, 이 때도 다른 요청을 기다린다.

요청한 서비스가 정보 요청 서비스인지를 판단한다.(218 단계) 즉, 서비스 요청이 네트워크 보안에 관련된 정보를 요청하는 서비스인 경우에는 해당 정보를 관리 콘솔부(130)로 제공한다.(220 단계)

서비스 요청이 프로세서 제어인 경우에는, 해당 프로세스를 제어하게 된다.(222 단계)

보안 에이전트부(126)는 상기의 서비스를 제공하기 위하여 통합관리시스템에서 제공하는 일부 인터페이스 프로그램과 관리를 위한 코드 부분을 포함한다.

통상, 보안 에이전트부(126)는 보안 시스템이 설치된 곳에 설치되나, 보안 레지스터부(134)가 위치한 곳이라면 통합관리시스템측에도 설치될 수 있다.

보안 레지스터부(134)는 관리 콘솔부(130)나 사용자의 입력에 의해 수행되며, 통합관리시스템에서 네트워크 보안 관련 자원의 효율적인 관리를 제공하기 위하여, 네트워크 보안에 관련된 정보를 상기 통합관리시스템과 보안 시스템의 공통 데이터 베이스에 저장하고, 상기 저장된 정보의 삭제, 수정 및 조회를 수행한다.

상기에서 저장된 정보는 통합관리시스템의 그래픽 인터페이스를 통하여 각 네트워크 보안 자원에 대한 접근 및 서비스를 할 수 있는 정보로 사용된다.

보안 레지스터부(134)는 상기의 기능을 수행하기 위하여 통합관리시스템에서 제공하는 일부 인터페이스 프로그램과 관련된 관리용 인터페이스를 위한 코드 부분을 포함한다.

로그 라우터부(136)는 상기 보안 시스템의 보안 서버(128)로부터 접속 시도에 대한 기록을 나타내는 로그 정보(Log Information)를 가져와서 분석하고, 문제가 있는 경우 긴급(Alert) 메시지 또는 SNMP(Single Network Management Protocol) 트랩 메시지를 통합관리시스템의 이벤트 콘솔(Event Console)로 제공한다.

로그 라우터부(136)는 통합관리시스템에서 제공하는 그래픽 인터페이스를 통하여 여러 노드에 분산되어 있는 네트워크 보안 자원 중 관리 콘솔부(130)와 통신하는 방식으로 동작한다. 통상, 관리 콘솔부(130)의 요청이나 사용자의 입력에 의해 동작을 개시하며, 보안 서버(128)로부터 각 접속 침입 시도를 알 수 있도록 로그 정보를 가져와서 분석하여 이를 통합관리시스템의 이벤트 콘솔부(132)로 전달하게 된다.

도 3에 로그 라우터부의 동작을 설명하는 흐름도가 도시되어 있다.

보안 서버(128)에 접속하여 로그 정보를 가져온다.(302, 304 단계)

로그 정보를 분석하고, 문제가 있는지를 판단한다.(306, 308 단계)

문제가 있으면, "긴급(Alert)" 메시지 또는 SNMP 트랩 메시지를 이벤트 콘솔부(132)로 보내게 된다.(310 단계)

문제가 없으면, 로그 정보를 통합관리시스템의 데이터 베이스(138)에 저장한다.(312 단계) 여기서, 문제가 없으면 바로 314 단계를 수행할 수도 있다.

분석할 다음 데이터가 있는지를 판단하여, 있으면 304 단계 이하를 반복수행한다.(314 단계)

로그 라우터부(136)는 상기의 기능을 수행하기 위하여 통합관리시스템의 일부 인터페이스 프로그램과 네트워크 보안 시스템의 인터페이스를 위한 코드 부분을 포함한다.

관리 콘솔부(130)는 SNMP를 사용하여 보안 시스템을 감시하며, 보안 관련 정보를 가져와서 상기 보안 시스템의 상태를 감시하고, 상기 보안 관련 정보 및 프로세서 제어를 상기 보안 에이전트부로 요청하며, 로그 라우터부(136) 및 보안 레지스터부(134)를 관리한다.

관리 콘솔부(130)는 이상에서 설명한 모듈들을 관리하고, 보조하는 도구로서 통합관리시스템이 설치되어 있는 시스템상에 함께 설치된다.

도 4에 관리 콘솔부의 동작을 나타내는 흐름도가 도시되어 있다.

서비스 종류를 체크한다.(402 단계)

SNMP 서비스인 경우에, SNMP를 사용하여 각 분산 노드들에 대한 네트워크 보안 자원을 감시한다.(404 단계) 즉, 네트워크 노드상에 분산되어 있는 네트워크 보안 자원들에 대한 정보를 공통 객체 저장부로부터 취합하고, 사용자가 등록한 별도의 정보를 통합하여 한눈에 네트워크 보안 자원들의 상태를 알 수 있도록 한다. 또한, 주기적으로 SNMP를 사용하여 각 네트워크 보안 자원들의 상태를 질의하고, 그 상태를 표시한다.

보안 정보 서비스인 경우에는, 보안 정보를 보안 에이전트부(126)로부터 가져와서 보안 서버(128)의 상태를 감시한다. 또한, 프로세스 제어 및 일부 정보를 보안 에이전트부(126)로 요청한다.(406 단계) 구체적으로는, 보안 에이전트부(126)와의 통신을 통하여 네트워크 보안 자원들의 상태를 표시한다. 또한, 보안 에이전트부(126)에게 네트워크 보안 자원에 대한 정보를 요청하고, 그 자원에 대한 프로세스 제어를 요청한다. 그리고, 독자적으로 네트워크 보안 서버(128)의 상태를 감시하고 일부 정보를 요청하는 작업을 수행한다. 이는 보안 에이전트부(126)가 정상적이지 못한 상태에서 특히 유용하다.

로그 라우팅 서비스인 경우에는, 로그 라우팅을 관리한다.(408 단계) 예컨대, 로그 라우터부 모듈의 시작과 끝을 지시한다. 또한, 로그 라우팅 서비스의 커맨드 라인의 실행을 대체하는 그래픽적인 사용환경을 제공함으로써, 사용자가 단지 마우스만을 이용하여 상기 로그 라우터부 모듈을 제어할 수 있도록 한다.

404, 406, 408 단계에서, 문제가 있는 경우 이벤트 콘솔부(132)로 그 상황을 전달한다. 예컨대, 보안 에이전트부(126)로부터의 트랩 메시지를 받고 그 내용에 따라 정보를 정보를 갱신하여, 그 내용을 통합관리시스템의 이벤트 콘솔부(132)로 전달한다.

보안 레지스터 서비스인 경우에는, 보안 레지스터를 관리한다. 410 단계) 예컨대, 보안 레지스터부 모듈의 시작과 끝을 지시한다. 마찬가지로, 보안 레지스터 모듈의 커맨드 라인 실행을 대체하는 그래픽적인 사용환경을 제공함으로써, 사용자가 단지 마우스만을 이용하여 상기 보안 레지스터 모듈을 제어할 수 있도록 한다

네트워크 보안 자원 정보를 공통 객체 저장부에 저장, 삭제, 수정 및 조회를 하도록 제어한다.(416 단계)

기타 서비스를 제공한다.(412 단계) 기타 서비스란 시스템에 대한 부가적인 서비스를 의미한다.

이외에, 관리 콘솔부(130)는 네트워크 보안 자원에 대해 그래픽 사용자 인터페이스(Graphic User Interface: GUI)의 클라이언트(Client) 프로그램을 수행할 수 있도록 하여 네트워크 보안 관리자들에게 좀 더 친숙하고 익숙한 환경을 제공한다. 상기 GUI 환경의 클라이언트는 보안 레지스터부(134) 모듈에 의해 공통 객체 저장부에 등록된 정보를 사용하여 통합관리시스템의 그래픽 인터페이스상에서도 수행할 수 있다.

본 발명은 상술한 실시예에 한정되지 않으며, 본 발명의 사상을 해치지 않는 범위내에서 당업자에 의한 변형이 가능함은 물론이다. 따라서, 본 발명에서 권리를 청구하는 범위는 상세한 설명의 범위내로 정해지는 것이 아니라 후술하는 청구범위로 한정될 것이다.

#### 발명의 효과

본 발명에 따르면, 상호 독립적으로 동작할 수 있는 4개의 모듈을 통합관리시스템 또는 보안시스템이 위치한 곳에 설치하여 상기 모듈들이 상호 작용하도록 함으로써 두 시스템을 통합하여 관리할 수 있도록 함으로써 다음과 같은 효과를 갖는다.

통합관리시스템과 보안시스템을 통합함으로써 현재 네트워크 보안 시스템 및 통합관리시스템을 독립적으로 또는 두 시스템을 별도로 운용하고 있는 사용자에게 자원의 효율적인 관리와 신뢰성 있는 사용환경을 제공할 수 있다.

따라서, 네트워크 보안 사용자로 하여금 통합관리시스템의 여러 자원들을 강력하고 효율적으로 관리할 수 있도록 하고, 통합관리시스템 사용자는 광범위하게 배치되어 있는 자원을 사용함에 있어 네트워크 보안의 강력하고 안전한 보안관리 기능을 제공받을 수 있다. 또한, 4개의 모듈을 상호 독립적으로 동작시킴으로써 각각들이 제공하는 기능들을 충분히 활용할 수 있다. 그리고, 보안에 대해 경증된 인터페이스를 제공하여 자원관리를 함으로써 기존의 통합관리시스템의 보안 문제점을 해결하였다.

#### (57) 청구의 범위

##### 청구항 1.

통합관리시스템(System Management System)과 보안시스템(Firewall System)을 통합하기 위한 시스템에 있어서,

상기 보안시스템의 네트워크 보안에 관련된 자원들의 상태를 감시하고, 정보를 수집하여 저장하며, 상기 보안시스템에 이상이 발생한 경우 트랩 이벤트를 발생하고, 상기 통합관리시스템의 요청에 따라 상기 네트워크 보안 관련 자원들에 대한 정보의 제공 또는 프로세스를 제어하기 위한 보안 에이전트부;

네트워크 보안에 관련된 정보를 상기 통합관리시스템과 보안시스템의 공동 데이터 베이스에 저장하고, 상기 저장된 정보의 삭제, 수정 및 조회를 수행하기 위한 보안 레지스터부;

상기 보안시스템으로부터 접속 시도에 대한 기록을 나타내는 로그 정보(Log Information)를 가져와서 분석하고, 문제가 있는 경우 긴급 메시지 또는 SNMP(Single Network Management Protocol) 트랩 메시지를 통합관리시스템의 이벤트 콘솔(Event Console)로 제공하기 위한 로그 라우터부; 및

상기 SNMP를 사용하여 상기 보안시스템을 감시하며, 상기 보안 관련 정보를 가져와서 상기 보안시스템의 상태를 감시하고, 상기 보안 관련 정보 및 프로세서 제어를 상기 보안 에이전트부로 요청하며, 상기 로그 라우터부 및 상기 보안 레지스터부를 관리하기 위한 관리콘솔부를 포함하며,

상기 보안 에이전트부, 보안 레지스터부, 로그 라우터부 및 관리 콘솔부는 통합관리시스템에서 제공하는 인터페이스 프로그램과 관련된 관리용 인터페이스를 위한 코드 또는 네트워크 보안 시스템의 인터페이스를 위한 코드를 포함함을 특징으로 하는 통합관리시스템과 보안시스템을 통합하기 위한 시스템.

##### 청구항 2.

제1항에 있어서, 상기 관리 콘솔부는

독자적으로 네트워크 보안 시스템의 상태를 감시하고 상기 보안에 관련된 정보를 상기 보안 에이전트부로 요청함을 특징으로 하는 통합관리시스템과 보안시스템을 통합하기 위한 시스템.

##### 청구항 3.

제1항에 있어서,

상기 보안 에이전트부는 보안시스템이 위치한 곳에 설치되며,

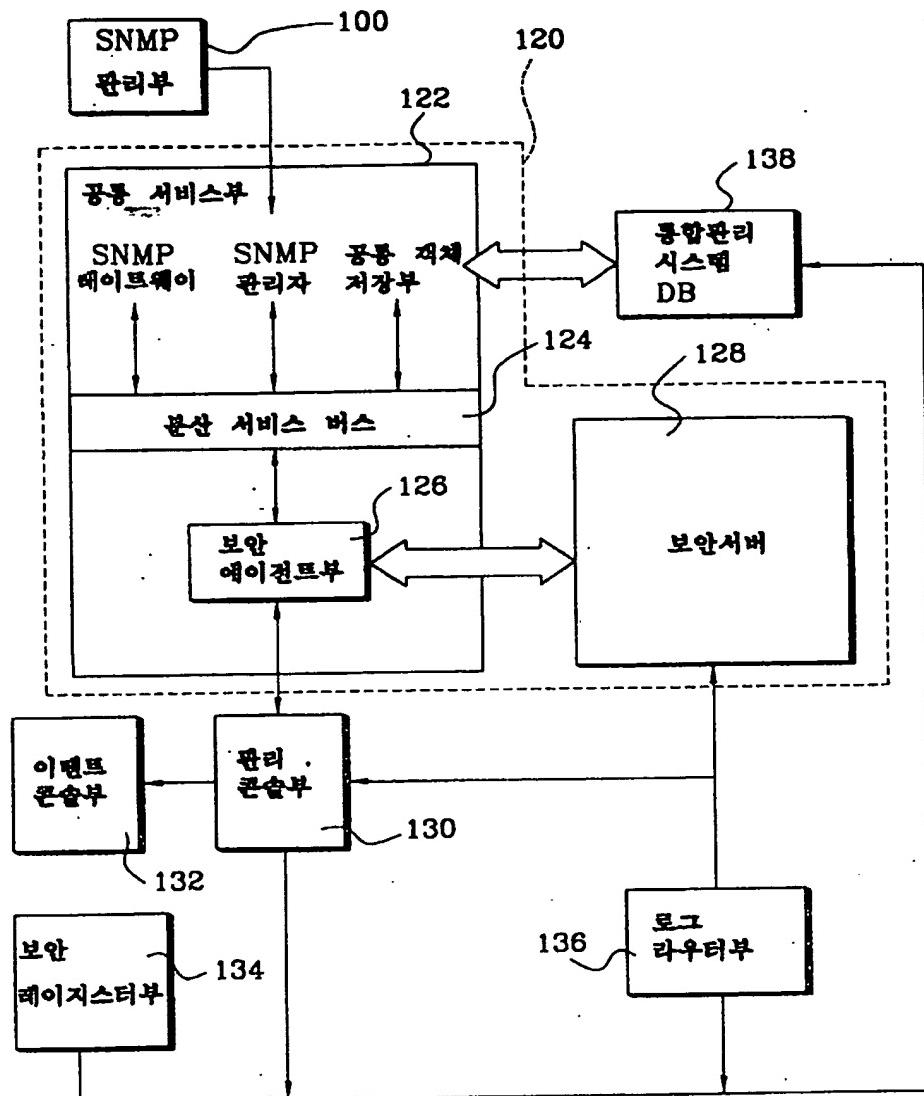
상기 보안 레지스터부, 로그 라우터부 및 관리 콘솔부는 통합관리시스템이 위치한 곳에 설치됨을 특징으로 하는 통합관리시스템과 보안시스템을 통합하기 위한 시스템.

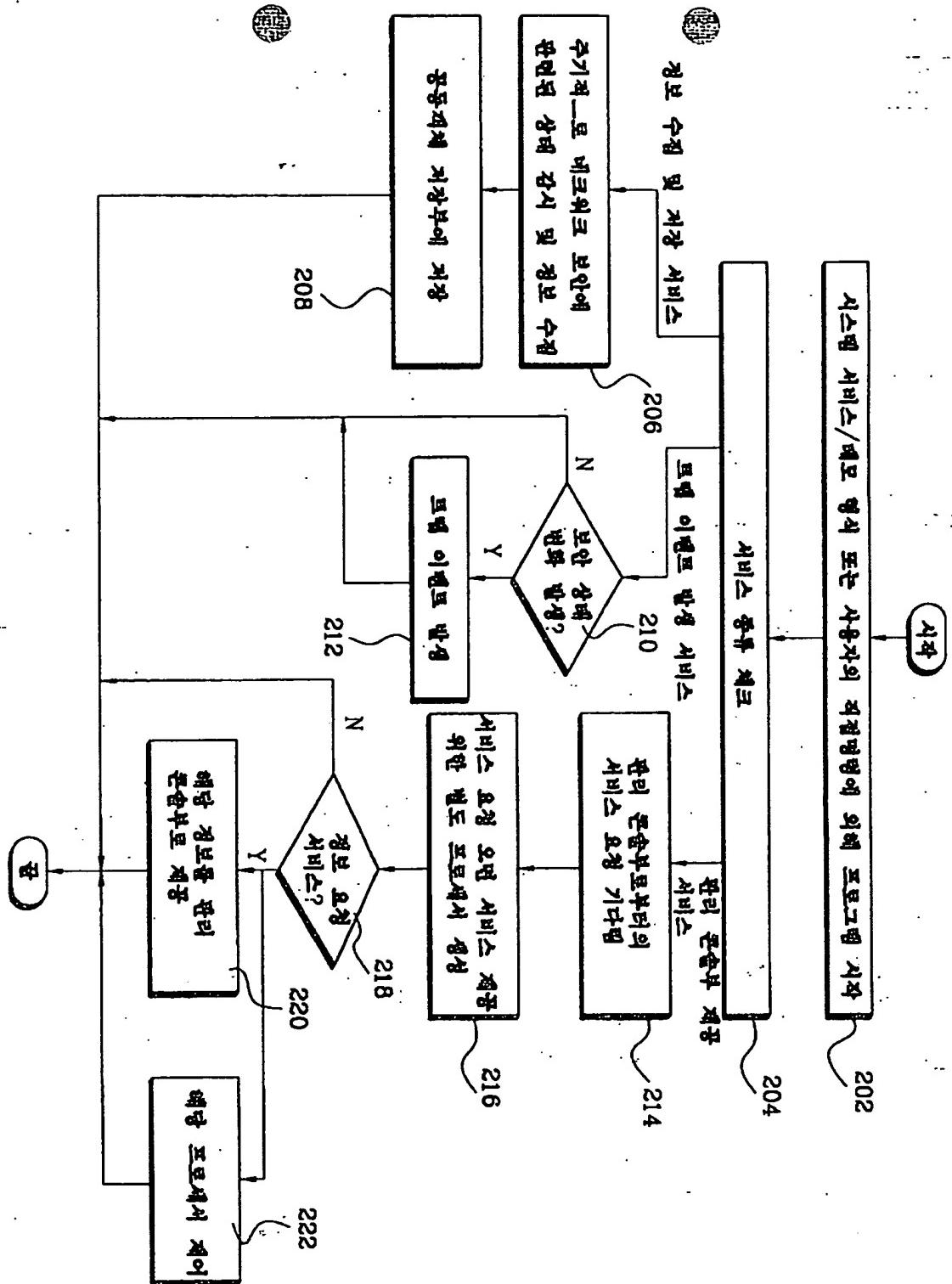
창구항 4.  
제1항에 있어서.

상기 보안 애이전트부와 상기 보안 레지스터부는 동일한 위치에 설치됨을 특징으로 하는 통합관리시스템과 보안시스템을 통합하기 위한 시스템

도면

도면 1





도면 3

